Beeld/add Trusted IPSec-certificaat op RV320 en RV325 VPN-routers

Doel

Certificaten worden gebruikt om de gebruikersidentiteit op een computer of internet te controleren en om een privégesprek of een beveiligd gesprek te verbeteren. In RV320 kunt u maximaal 50 certificaten toevoegen door zelf-ondertekening of toestemming van derden. U kunt een certificaat voor een client of voor een beheerder exporteren, slaat u dat op een pc of USB-poort en importeert u dat vervolgens. IPsec wordt gebruikt in de uitwisseling van gegevens over sleutelproductie en authenticatie, het protocol voor het vaststellen van de sleutelpositie, encryptie algoritme of authenticatiemechanisme voor veilige authenticatie en validatie van online transacties met SSL-certificaten.

Dit artikel legt uit hoe u Trusted IPSec-certificaat kunt bekijken en toevoegen op de RV32x VPN-routerserie.

Toepasselijke apparaten

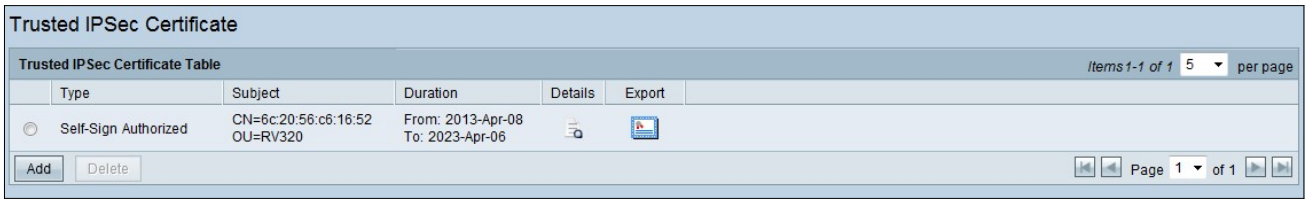
- RV320 VPN-router met dubbel WAN
- RV325 Gigabit VPN-router met dubbel WAN

Softwareversie

- v1.1.0.09

Trusted IPSec-certificaat

Stap 1. Meld u aan bij het web-configuratieprogramma en kies **het certificaatbeheer > Trusted IPSec-certificaat**. De pagina *Trusted IPSec*-certificaat wordt geopend:



De *Trusted IPSec*-pagina bevat de volgende velden:

- Type — Er zijn twee soorten certificaten beschikbaar

- Zelfondertekend — Het is een Secure Socket Layer (SSL)-certificaat dat door zijn eigen schepper is ondertekend. Het is minder betrouwbaar omdat het niet kan worden geannuleerd als de privé-sleutel op een of andere manier door de aanvaller op het spel wordt gezet.

- Aanvraag voor gecertificeerde signalering — Het is een openbare sleutelinfrastructuur (PKI) die naar de certificeringsinstantie wordt gestuurd om een digitaal identiteitsbewijs aan te vragen. Het is veiliger dan door zichzelf getekend te worden, omdat de privé-sleutel geheim gehouden wordt.

- Onderwerp — Het toont aan aan wie het certificaat is afgegeven.

- Duur — Het geeft de datum aan waarop het certificaat verstrijkt. De beveiliging van de website kan niet worden gegarandeerd indien deze datum is overschreden.

- Details — Het geeft alle details weer over de certificaatuitgifte, het certificaatserienummer en de vervaldatum die door de CA-dienst zijn gegenereerd. De informatie wordt gebruikt wanneer een Generate certificaatSigning Aanvraag wordt gecreëerd en naar uw CA dienst voor validatie wordt verzonden.

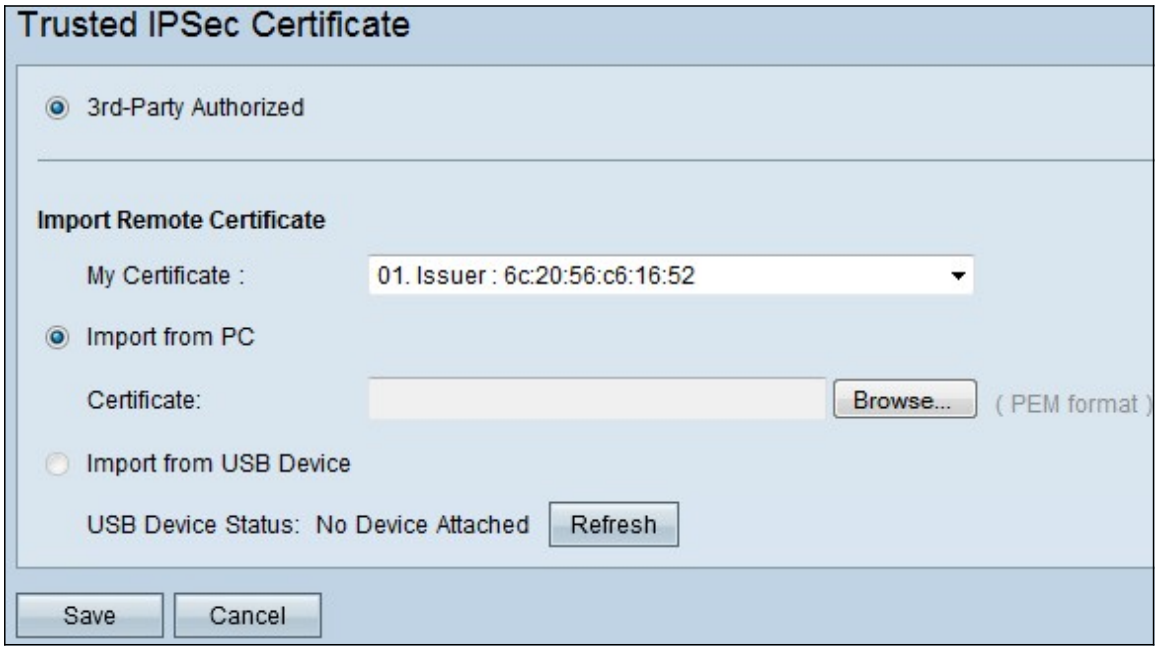
- Exporteren — Klik op het pictogram Exporteren om een certificaat te exporteren of weer te geven. Het pop-upvenster toont waar u het certificaat voor inspectie kunt openen of het certificaat op een pc kunt opslaan.

Stap 2. Klik op het aanvinkvakje **Enable** om een bepaald IPSec-certificaat in te schakelen.

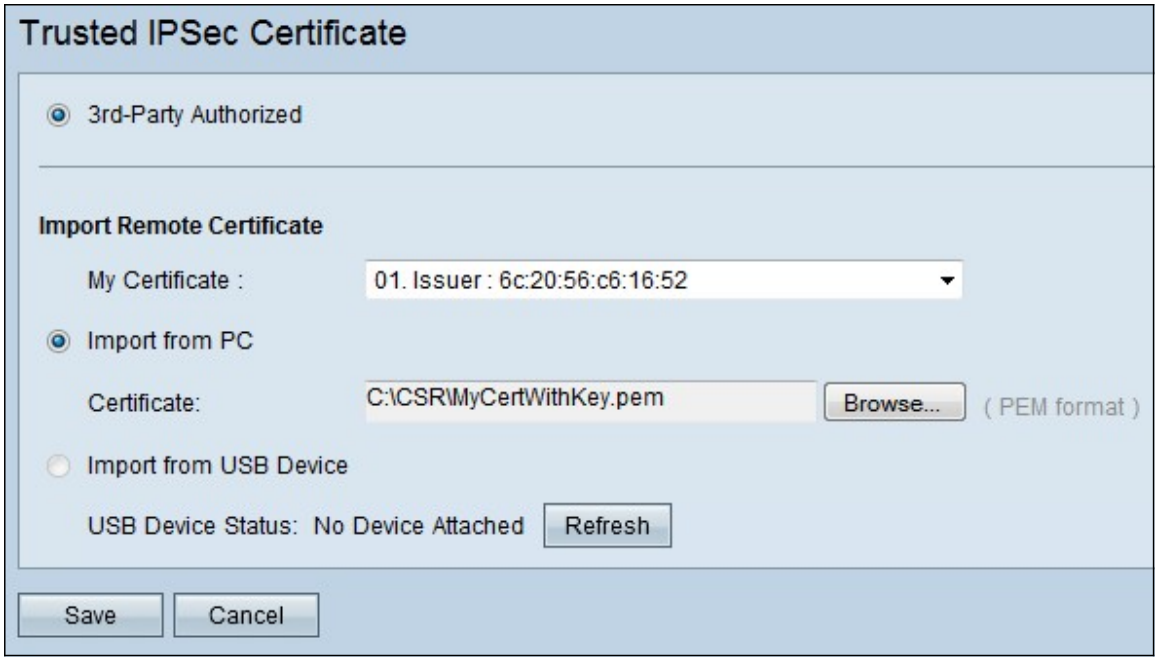
Stap 3. Klik op **Add** om een nieuw certificaat te krijgen van de PC of USB.

- Importeren vanuit een pc - U kunt het certificaat vinden en importeren naar het apparaat

- Importeren vanuit USB — Van het USB-apparaat dat op het apparaat is aangesloten, kunt u het certificaat ook importeren.



Stap 3. Klik op **Bladeren** om het CA-certificaat vanaf de pc te vinden.



Stap 4. Klik op **Save** om het certificaat aan de vertrouwde tabel met IPSec-certificaten toe te voegen.